arXiv:1003.4393v2 [math.NT] 3 Apr 2010

Shafarevich-Tate groups of elliptic curves upon quadratic extension and several applications

Derong Qiu *

(School of Mathematical Sciences, Institute of Mathematics and Interdisciplinary Science, Capital Normal University, Beijing 100048, P.R.China)

Abstract Let E be an elliptic curve over a number field F and $K = F(\sqrt{D})$ be a quadratic extension of F. In this paper, for E and its quadratic $D-$twist E_D, by calculating the cohomology groups, we obtain an explicit formula relating the orders of the Shafarevich-Tate groups $Ш\,(E/F), Ш\,(E_D/F), Ш\,(E/K)$ and the ranks of the groups of $F-$rational points of E and E_D. Then, assuming the finiteness of Shafarevich-Tate groups, we prove by a simple way different from the recent paper [Dok] that each square free positive integer $n \equiv 5, 6$ or $7(\mathrm{mod} 8)$ is a congruent number; and for several families of elliptic curves $E_n : y^2 = x^3 - n^2x$, we prove that the orders of $Ш(E_n/\mathbb{Q}(\sqrt{n}))(\cong Ш(E_1/\mathbb{Q}(\sqrt{n})))$ are equal to the squares of a product of $2-$th powers with the n(or $n/2$)$-$th Fourier coefficients of some modular forms of weight $3/2$. In particular, unconditionally, we obtain the values of $Ш\,(E/\mathbb{Q}(\sqrt{D}))$ for some elliptic curves E and integers D, e.g., we show that all $Ш\,(E/\mathbb{Q}(\sqrt{D}))$ are trivial for the elliptic curve E of conductor 37 and the 23 integers D in Kolyvagin's papers.

Keywords: Elliptic curve, Shafarevich-Tate group, Birch and Swinnerton-

* E-mail: derong@mail.cnu.edu.cn

Dyer conjecture, congruence number problem, Heegner point, cohomology group.

2000 Mathematics Subject Classification: 14H52 (primary), 11G05, 11G20, 11G40, 14G10, 14K22 (Secondary).

1. Introduction and statement of main results

Let F, K be number fields with $K = F(\sqrt{D})$ a quadratic extension of F for some $D \in F^*\backslash F^{*^2}$. Let $G = \mathrm{Gal}(K/F) =< \sigma >$ be its Galois group with a generator σ. Let E be an elliptic curve defined over F and E_D be its quadratic $D-$twist (see Section 2 below). By the Mordell-Weil Theorem (see [Si1]), the group $E(F)$ of $F-$rational points of E is a finitely generated abelian group, so are the groups $E_D(F)$ and $E(K)$. For simplicity, in the following, we denote $r_F = \mathrm{rank}E(F)$, $r_{D,F} = \mathrm{rank}E_D(F)$ and $r_K = \mathrm{rank}E(K)$. Let Ш (E/F), Ш (E_D/F) and Ш (E/K) be the Shafarevich-Tate groups of E over F, E_D over F and E over K respectively (see [Si1] for the definition).

Throughout this paper, for a set S, we denote its cardinal by $\sharp S$. For arbitrary abelian group A and positive integer m, we denote $mA = \{ma : \ a \in A\}$ and $A[m] = \{a \in A : \ ma = 0\}$. If A is a $G-$module, then one has the following Tate cohomology groups :

$$\widehat{\mathrm{H}}^n(G, A) = \mathrm{H}^n(G, A) \quad \text{if } n \geq 1; \qquad \widehat{\mathrm{H}}^0(G, A) = A^G/(1+\sigma)A.$$

For the basic facts of cohomology groups $\mathrm{H}^n(G, A)$ $(0 \leq n \in \mathbb{Z})$ and Tate cohomology groups $\widehat{\mathrm{H}}^m(G, A)$ $(m \in \mathbb{Z})$ of $G-$module A, see [Se, part three] and [AW].

In this paper, firstly, by calculating the Herbrand quotients, we obtain the order of $\mathrm{H}^1(G, E(K))$ as follows:

Theorem A (see Theorem 2.5 below).

$$\sharp \mathrm{H}^1(G, E(K)) = 2^{r_{D,F}-r_F} \cdot (E(F) : N_D(F)).$$

Depending on this conclusion, then by the results of Yu and Gonzalez-Aviles (see [Y], [GA]) on the Shafarevich-Tate groups of abelian varieties over Galois extensions, and the results of Mazur, Kramer and Tunnell (see [Ma], [Kr] [KT]) on local norm indices, we obtain the following formula relating the orders $\sharp Ш(E/F), \sharp Ш(E_D/F), \sharp Ш(E/K)$ and the ranks $r_F, r_{D,F}$.

Theorem B (see Theorem 3.2 below).

Assume that the Shafarevich-Tate groups are finite. Then

$$\frac{\sharp Ш(E/F) \cdot \sharp Ш(E_D/F)}{\sharp Ш(E/K)} = 2^{r_{D,F}-r_F-\delta(E,F,K)} \cdot (E(F) : N_D(F))^2,$$

where $\delta(E, F, K)$ is the MKT index of E over K/F (see Def.3.1. below).

Corollary C. Assume that the Shafarevich-Tate groups are finite. Then

$$r_K \equiv r_{D,F} - r_F \equiv \delta(E, F, K) \pmod 2.$$

Proof. By a well known theorem of Cassels (see [Si 1], chapt.X, Thm.4.14), the orders $\sharp Ш(E/F), \sharp Ш(E_D/F)$ and $\sharp Ш(E/K)$ are perfect squares. So the congruences follow from the above Theorem B and the fact that $r_K = r_F + r_{D,F}$ (see [ABF],[RS]). The proof is completed. $\square$

Let $L(E/F, s)$ be the Hasse-Weil $L-$function of the elliptic curve E over F, then the Birch and Swinnerton-Dyer conjecture says

Conjecture (Birch, Swinnerton-Dyer)

(BSD 1) $\mathrm{ord}_{s=1}L(E/F,s)=r_F$;

(BSD 2) $\displaystyle\lim_{s\to 1}\frac{L(E/F,s)}{(s-1)^{r_F}}=\Omega_{E/F}\times \mathrm{Reg}_{\infty,F}(E)\times\frac{\sharp\,\text{Ш}(E/F)\prod_{v\in M_F}c_v}{\sqrt{d(F)}\times\sharp E(F)^2_{\mathrm{tors}}}$.

(see [D, chapt.I] for a detailed statement and explanation). In the following, for convenience, we call it the full BSD conjecture. As in [D], we denote

$$(\mathrm{BSD})_{\infty,F}(E)=\mathrm{Reg}_{\infty,F}(E)\times\frac{\sharp\,\text{Ш}(E/F)\prod_{v\in M_F}c_v}{\sqrt{d(F)}\times\sharp E(F)^2_{\mathrm{tors}}}.$$

Another related important conjecture is the following Shafarevich-Tate conjecture

Shafarevich-Tate Conjecture. Each Ш (E/F) is a finite group.

A weak form of the BSD conjecture says that $L(E/F,1)=0$ if and only if $E(F)$ is an infinite group. For a square free positive integer $n\equiv 5,6$ or $7(\mathrm{mod} 8)$, it is well known that if the weak BSD conjecture holds for the elliptic curve $E_n: y^2=x^3-n^2x$, then n is a congruent number (see [Kob], p.92), and a theorem of Tunnell gives an almost complete solution of the famous congruent number problem if the weak form of the BSD conjecture is true (see [T] and [Kob]). By using the above Theorem B, we obtain several results about the ranks of the elliptic curves E_n and the congruent number problem as follows:

Theorem D (see Theorem 4.3 below).

Let n be a square free integer satisfying one of the following conditions

(1) $n>0$ and $n\equiv 5,6$ or 7 (mod 8); (2) $n<0$ and $n\equiv 1,2$ or 3 (mod 8).

Then for the elliptic curves $E=E_1: y^2=x^3-x$ and E_n as above, if both Ш $(E_n/\mathbb{Q})$ and Ш $(E/\mathbb{Q}(\sqrt{n}))$ are finite, we have

$$\mathrm{rank}(E(\mathbb{Q}(\sqrt{n})))=\mathrm{rank}(E_n(\mathbb{Q}))\equiv 1\ (\mathrm{mod}\ 2).$$

In particular, both $E(\mathbb{Q}(\sqrt{n}))$ and $E_n(\mathbb{Q})$ are infinite groups.

Corollary E. Assume that the Shafarevich-Tate conjecture is true. Then each square free positive integer $n \equiv 5, 6$ or $7 \pmod 8$ is a congruent number.

Proof. It is well known that n is a congruent number if and only if $E_n(\mathbb{Q})$ has non-zero rank (see [Kob], p.46), and then the conclusion follows from the above Theorem D. The proof is completed. $\square$

Remark. After this paper finished, in an email on March 24, 2010, Professor John Coates kindly told the author the following fact: Tim and Vladimir Dokchitser proved several years ago in [Dok] the parity conjecture for all elliptic curves over $\mathbb{Q}$ and all primes p. Thus, if assume the finiteness of the $p-$primary part of Ш for one prime p, their result will imply that E_n with $n \equiv 5, 6$ or $7 \pmod 8$, has a $\mathbb{Q}-$point of infinite order.

This result is stronger than those of the above Theorem D and Corollary E, meanwhile, the method here is different and simple.

It is well known that the $L-$ function $L(E/\mathbb{Q}, s) = \sum b_m m^{-s}$ of the elliptic curve $E = E_1 : y^2 = x^3 - x$ corresponds to a weight two cusp form $g = \sum b_m q^m \in S_2(\Gamma_0(32))$ (see [Kob], p.217), and for the elliptic curve E_n, by Tunnell's theorem (see [T] or [Kob, p.217]), there exist a form $f = \sum a_m q^m \in S_{3/2}(\widetilde{\Gamma}_0(128))$ and a form $f' = \sum a'_m q^m \in S_{3/2}(\widetilde{\Gamma}_0(128), \chi_2)$ such that their Shimura lifts Shimura$(f) =$ Shimura$(f') = g$ and

$$L(E_n/\mathbb{Q}, 1) = \begin{cases} \frac{\omega}{4\sqrt{n}} a_n^2 & \text{if } n \text{ is odd,} \\ \frac{\omega}{2\sqrt{n}} (a'_{n/2})^2 & \text{if } n \text{ is even.} \end{cases}$$

where $\omega = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} = 2.6220575$ is the least positive period of $E/\mathbb{Q}$.

By using the formula in Theorem B above, we obtain some results of

Ш $(E/\mathbb{Q}(\sqrt{n}))$ and the full BSD conjecture for E over $\mathbb{Q}(\sqrt{n})$ as follows:

Theorem F (see Theorem 4.4 below).

Let n be a square free integer satisfying one of the following conditions

(1) $n > 0$ and $n \equiv 1, 2$ or $3 \pmod 8$; (2) $n < 0$ and $n \equiv 5, 6$ or $7 \pmod 8$.

Then for the elliptic curves $E = E_1 : y^2 = x^3 - x$ and E_n as above, if the full BSD conjecture is true for E_n over $\mathbb{Q}$ with $L(E_n/\mathbb{Q}, 1) \neq 0$, and Ш $(E/\mathbb{Q}(\sqrt{n}))$ is finite, we have

$$\sharp\, Ш(E/\mathbb{Q}(\sqrt{n})) = \begin{cases} 2^{-4} \cdot a_n^2 & \text{if } n > 0 \text{ and } n \equiv 1 \pmod 8, \\ 2^{-2} \cdot a_n^2 & \text{if } n > 0 \text{ and } n \equiv 3 \pmod 8, \\ 2^{-2} \cdot (a'_{n/2})^2 & \text{if } n > 0 \text{ and } n \equiv 2 \pmod 8, \\ 2^{-2} \cdot a_{-n}^2 & \text{if } n < 0 \text{ and } n \equiv 5 \text{ or } 7 \pmod 8, \\ (a'_{-n/2})^2 & \text{if } n < 0 \text{ and } n \equiv 6 \pmod 8, \end{cases}$$

where $a_{|n|}$ and $a'_{|n/2|}$ are the Fourier coefficients of the above modular forms f and f'. Moreover, the full BSD conjecture is true for E over the quadratic field $\mathbb{Q}(\sqrt{n})$.

Remark. (1) Note that E and E_n are isomorphic over $\mathbb{Q}(\sqrt{n})$, and $E_n = E_{-n}$, so in particular $\sharp\, Ш(E_n/\mathbb{Q}(\sqrt{\pm n})) = \sharp\, Ш(E/\mathbb{Q}(\sqrt{\pm n}))$, and one has all the same results for E_n over $\mathbb{Q}(\sqrt{n})$ as E in the above Theorem F. Moreover, the Fourier coefficients a_n and a'_n $(n > 0)$ can be determined by the number of solutions of some concrete quadratic forms in three variables (see Tunnell's theorem in [T] for the detail).

(2) For E and E_n in the Theorem F above, it seems from the proof of Theorem 4.4 below that the ratio $\sharp\, Ш(E/\mathbb{Q}(\sqrt{n}))/\sharp\, Ш(E_n/\mathbb{Q})$ may be possibly arbitrarily

large, for example, for a square free positive integer $n \equiv 1 \pmod 8$, then under our assumption, one has $\sharp\,\text{Ш}(E/\mathbb{Q}(\sqrt{n}))/\sharp\,\text{Ш}(E_n/\mathbb{Q}) = 2^{2\omega_0(n)-4}$, where $\omega_0(n)$ is the number of odd prime divisors of n.

Example G. For the elliptic curves $E_n : y^2 = x^3 - n^2x$ and $E = E_1$ as above, assume that Ш $(E/\mathbb{Q}(\sqrt{n}))$ is finite.

(1) If $n = \pm p,\ p$ is a prime number, and $p \equiv 3 \pmod 8$, then

$$\sharp\,\text{Ш}(E/\mathbb{Q}(\sqrt{p})) = \sharp\,\text{Ш}(E/\mathbb{Q}(\sqrt{-p})) = \frac{1}{4}a_p^2,$$

in particular, all such a_p are even. Moreover, the full BSD conjecture is true for E over both $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-p})$.

(2) Suppose $n = \pm p_1 \cdots p_m \equiv 1 \pmod 4$, where $p_1, \cdots, p_m$ are distinct prime numbers with $p_i \not\equiv 5 \pmod 8$. If $s_k(n) = 1$, then

$$\sharp\,\text{Ш}(E/\mathbb{Q}(\sqrt{n})) = \begin{cases} 2^{-4} \cdot a_n^2 & \text{if } n > 0 \text{ and } n \equiv 1 \pmod 8, \\ 2^{-2} \cdot a_{-n}^2 & \text{if } n < 0 \text{ and } n \equiv 5 \pmod 8. \end{cases}$$

(3) Suppose $n = p_1 \cdots p_m$, where $p_1, \cdots, p_m$ are distinct prime numbers with $p_1 \equiv 3 \pmod 8$ and $p_2 \equiv \cdots \equiv p_m \equiv 1 \pmod 8$. If $s_{2m-1}(-n) = 1$, then

$$\sharp\,\text{Ш}(E/\mathbb{Q}(\sqrt{n})) = 2^{-2} \cdot a_n^2, \text{ in particular, } 2^m \parallel a_n, \ \textit{i.e.}, \ v_2(a_n) = m.$$

Moreover, the full BSD conjecture is true for E over $\mathbb{Q}(\sqrt{n})$ in cases (2) and (3). Here $s_k(n)$ and $s_{2m-1}(-n)$ are the $\mathbb{F}_2-$valued functions on n and its Gaussian prime factors defined in [Z].

Proof. (1). By a theorem of Rubin (see [R2], P.26), the full BSD conjecture is true for $E_p : y^2 = x^3 - p^2x$ over $\mathbb{Q}$ and $L(E_p/\mathbb{Q}, 1) \neq 0$, so the conclusion follows directly from the above Theorem F.

(2) and (3). By the Theorem 2 and Proposition 3 in [Z], the full BSD conjecture is true for $E_n : y^2 = x^3 - n^2x$ over $\mathbb{Q}$ and $L(E_n/\mathbb{Q}, 1) \neq 0$ in these cases, so the conclusion of the orders of the Shafarevich-Tate groups and the full BSD conjecture for E over $\mathbb{Q}(\sqrt{n})$ follows directly from the above Theorem F. Now we come to compute the 2−adic valuation of a_n in case (3). In fact, by the Theorem 2 in [Z], we know that, if $s_{2m-1}(-n) = 1$, then $L(E_n/\mathbb{Q}, 1) \neq 0$ and the 2−Selmer group $S^{(2)}(E_n/\mathbb{Q})$ has order 4. So by a theorem of Coates-Wiles (see [CW]), one has $r_{n,\mathbb{Q}} = \mathrm{rank} E_n(\mathbb{Q}) = 0$, so $E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \cong E_n(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. Then by the exact sequence (see [Si1], chapt. X, Thm. 4.2)

$$0 \to E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \to S^{(2)}(E_n/\mathbb{Q}) \to Ш\,(E_n/\mathbb{Q})[2] \to 0$$

we get $Ш\,(E_n/\mathbb{Q})[2] = 0$, hence the 2−primary part $Ш\,(E_n/\mathbb{Q})[2^\infty] = 0$, and so $\sharp\, Ш(E_n/\mathbb{Q})$ is odd. But, from the fact that the full BSD conjecture for E_n over $\mathbb{Q}$, it is easy to know that $\sharp\, Ш(E_n/\mathbb{Q}) = 2^{-2m}a_n^2$ (see the proof of Theorem 4.4 below), so $v_2(a_n) = m$. The proof is completed. $\square$

Lastly, we give a result of the Shafarevich-Tate groups related to the Heegner points as follows:

Theorem H (see Theorem 5.1 below).

(1) Let E be an elliptic curve defined over $\mathbb{Q}$, and $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field satisfying the Heegner hypothesis. Let P_K be a Heegner point of $E(K)$, if P_K is of infinite order, then

$$\frac{\sharp\, Ш(E/\mathbb{Q}) \cdot \sharp\, Ш(E_D/\mathbb{Q})}{\sharp\, Ш(E/K)} = \begin{cases} 2^{1-\delta_\infty-\delta_g} \cdot (E(\mathbb{Q}) : N_D(\mathbb{Q}))^2 & \text{if } L(E/\mathbb{Q}, 1) \neq 0, \\ 2^{-1-\delta_\infty-\delta_g} \cdot (E(\mathbb{Q}) : N_D(\mathbb{Q}))^2 & \text{if } L(E/\mathbb{Q}, 1) = 0. \end{cases}$$

(2) For the elliptic curve $E : y^2 = x^3 - x + \frac{1}{4}$ and the imaginary quadratic field

$K=\mathbb{Q}(\sqrt{D})$ satisfying the Heegner hypothesis, if the Heegner point $P_K \in E(K)$ is of infinite order, then

$$\sharp\,\text{Ш}(E/K) = 2^{\delta_g} \cdot \sharp\,\text{Ш}(E_D/\mathbb{Q}).$$

In particular, for each $D \in \{-7, -11, -47, -71, -83, -84, -127, -159, -164, -219, -231, -263, -271, -287, -292, -303, -308, -359, -371, -404, -443, -447, -471\}$, the group $\text{Ш}\,(E/K)$ is trivial.

By these methods, one can obtain other similar examples as done in Example G and Theorem H above.

2. Quadratic twists and cohomology groups

Let F, K be number fields with $K = F(\sqrt{D})$ a quadratic extension of F for some $D \in F^* \setminus F^{*2}$. Let $G = \mathrm{Gal}(K/F) =<\sigma>$ be its Galois group with a generator σ. Then $\sigma^2 = \;\mathrm{id}$ and $\sigma(\sqrt{D}) = -\sqrt{D}$. Let $E:\; y^2 = x^3 + ax + b$ be an elliptic curve defined over F, i.e., $a, b \in F$. Its quadratic $D-$twist is given by $E_D:\; y^2 = x^3 + aD^2x + bD^3$ (see [Si1]). Since E and E_D are $K-$isomorphic as given by

$$\phi_D:\; E_D \longrightarrow E, \quad (x,y) \longmapsto \left(\frac{x}{(\sqrt{D})^2}, \frac{y}{(\sqrt{D})^3}\right),$$

we have $E(K) \cong E_D(K)$, $\text{Ш}\,(E_D/K) \cong \text{Ш}\,(E/K)$ and $r_F + r_{D,F} = r_K$ (see [ABF], [RS]). Denote

$$R_D(F) = \phi_D(E_D(F)) = \left\{\left(\frac{x}{D}, \frac{y}{(\sqrt{D})^3}\right):\; (x,y) \in E_D(F)\right\} \cup \{O\} \subset E(K).$$

Obviously, $R_D(F)$ is a subgroup of $E(K)$, and $R_D(F) \cong E_D(F)$ as abstract groups.

Lemma 2.1. $R_D(F) = \{P \in E(K):\; \sigma(P) = -P\}$.

Proof. Let $O \neq P \in R_D(F)$, then $P = (\frac{x}{D}, \frac{y}{D\sqrt{D}})$ for some $(x, y) \in E_D(F)$. So $\sigma(P) = (\frac{x}{D}, \frac{y}{-D\sqrt{D}}) = -(\frac{x}{D}, \frac{y}{D\sqrt{D}}) = -P$. Conversely, if $O \neq P = (x, y) \in E(K)$ satisfying $\sigma(P) = -P$, then $(\sigma x, \sigma y) = (x, -y)$, so $\sigma x = x$ and $\sigma y = -y$, and then $x \in F$. Since $y \in K$, we may write $y = s + t\sqrt{D}$ with $s, t \in F$. By $\sigma(s + t\sqrt{D}) = -(s + t\sqrt{D})$ we get $s = 0$, which implies $y = t\sqrt{D}$. Obviously, $(Dx, tD^2) \in E_D(F)$, hence $P = (x, t\sqrt{D}) = \phi_D(Dx, tD^2) \in \phi_D(E_D(F)) = R_D(F)$. This proves Lemma 2.1. $\square$

It is easy to see that the two maps

$$\varphi_1 : \ E(K) \longrightarrow E(K), \quad P \longmapsto P + \sigma P \quad (\forall P \in E(K)) \quad \text{and}$$

$$\varphi_2 : \ E(K) \longrightarrow E(K), \quad P \longmapsto P - \sigma P \quad (\forall P \in E(K))$$

are endomorphisms of abelian group $E(K)$ with kernels $\ker\varphi_1 = R_D(F)$ (by Lemma 2.1) and $\ker\varphi_2 = E(F)$ respectively. We denote $N_D(F) = \mathrm{im}\varphi_1$, the images of φ_1; and $T_D(F) = \mathrm{im}\varphi_2$, the images of φ_2. Obviously $N_D(F), T_D(F)$ and $R_D(F)$ are finitely generated abelian groups because they are subgroups of $E(K)$ (see [L2]). We have

$$2E(F) \subset N_D(F) \subset E(F), \quad 2R_D(F) \subset T_D(F) \subset R_D(F).$$

Moreover, by the former discussion and the following exact sequences of abelian groups

$$O \longrightarrow R_D(F) \longrightarrow E(K) \longrightarrow^{\varphi_1} N_D(F) \longrightarrow O \quad \text{and}$$

$$O \longrightarrow E(F) \longrightarrow E(K) \longrightarrow^{\varphi_2} T_D(F) \longrightarrow O, \quad \text{we get}$$

$$\mathrm{rank}E(K) = \mathrm{rank}R_D(F) + \mathrm{rank}N_D(F) = \mathrm{rank}E(F) + \mathrm{rank}T_D(F),$$

$$\mathrm{rank}T_D(F) = \mathrm{rank}E_D(F) = \mathrm{rank}R_D(F), \quad \mathrm{rank}N_D(F) = \mathrm{rank}E(F).$$

In particular, the quotient groups $E(F)/N_D(F)$ and $R_D(F)/T_D(F)$ are finite abelian groups.

Lemma 2.2.

(1) $R_D(F)[2] = R_D(F) \cap E(F) = E(F)[2]$.

(2) $T_D(F)[2] = T_D(F) \cap E(F) = T_D(F)^G \subset R_D(F)^G = E(F)[2]$.

(3) The inverse images of $2R_D(F), 2E(F)$ under φ_2, φ_1 respectively are given by $\varphi_2^{-1}(2R_D(F)) = E(F) + R_D(F) = \varphi_1^{-1}(2E(F))$.

Proof. (1) Let $P \in E(F)[2]$, then $2P = O$ and $\sigma P = P$, so $\sigma P = P = -P$, by Lemma 2.1, $P \in R_D(F)$. So $E(F)[2] \subset R_D(F)[2]$ and $E(F)[2] \subset R_D(F) \cap E(F)$. Now let $P \in R_D(F)[2]$, by Lemma 2.1, $P \in E(K), \sigma P = -P$ and $2P = O$. So $P \in E(F)[2]$. Hence $R_D(F)[2] \subset E(F)[2]$ and so $R_D(F)[2] = E(F)[2]$. Lastly, let $P \in R_D(F) \cap E(F)$, then $P = \sigma P = -P$, so $2P = O$ and then $P \in E(F)[2]$. Hence $R_D(F) \cap E(F) \subset E(F)[2]$ and so $R_D(F) \cap E(F) = E(F)[2]$. This proves (1).

(2) For $P \in T_D(F)$, we have $P = Q - \sigma Q = 2Q - (Q + \sigma Q)$ for some $Q \in E(K)$. Then it is easy to see that $2P = 0 \Leftrightarrow P \in T_D(F)^G \Leftrightarrow 2Q \in E(F) \Leftrightarrow P \in E(F)$. Hence $T_D(F)[2] = T_D(F) \cap E(F) = T_D(F)^G$. On the other hand, by definition, $T_D(F)^G \subset R_D(F)^G = E(F)[2]$. This proves (2).

(3) For $P \in E(F) + R_D(F)$, we have $P = P_0 + Q_0$ with $P_0 \in E(F)$ and $Q_0 \in R_D(F)$. By Lemma 2.1, $\sigma Q_0 = -Q_0$, so by definition, $\varphi_2(P) = \varphi_2(P_0 + Q_0) = P_0 + Q_0 - \sigma(P_0 + Q_0) = 2Q_0 \in 2R_D(F)$, hence $P \in \varphi_2^{-1}(2R_D(F))$. This implies $E(F) + R_D(F) \subset \varphi_2^{-1}(2R_D(F))$.

Conversely, for $P \in \varphi_2^{-1}(2R_D(F))$, we have $\varphi_2(P) = 2Q$ for some $Q \in R_D(F)$. By Lemma 2.1, $Q + \sigma Q = O$, so by definition, $P - \sigma P = \varphi_2(P) = 2Q = Q - \sigma Q$, i.e.,

$P-Q=\sigma(P-Q)$, so $P-Q\in E(F)$, and then $P\in Q+E(F)\subset R_D(F)+E(F)$. This implies $\varphi_2^{-1}(2R_D(F))\subset E(F)+R_D(F)$. Therefore, $\varphi_2^{-1}(2R_D(F))=E(F)+R_D(F)$. One can similarly prove that $\varphi_1^{-1}(2E(F))=E(F)+R_D(F)$. This proves (3), and the proof of Lemma 2.2 is completed. $\square$

Lemma 2.3.

$(E(K):E(F)+R_D(F))=(T_D(F):2R_D(F))=(N_D(F):2E(F))$.

Proof. Let $A=E(K), B=E(F)+R_D(F), f=\varphi_1$, then by Lemma 2.2 and the formula of norm index (see [L 1], pp. 46, 179)

$$(A:B)=(A^f:B^f)(A_f:B_f)$$

we get $(E(K):E(F)+R_D(F))=(\varphi_1(E(K)):\varphi_1(E(F)+R_D(F)))(\ker\varphi_1:\ker\varphi_1\mid_B)=(N_D(F):2E(F))\cdot(R_D(F):R_D(F))=(N_D(F):2E(F))$. By taking $f=\varphi_2$ we can similarly obtain that $(E(K):E(F)+R_D(F))=(T_D(F):2R_D(F))$. This proves Lemma 2.3. $\square$

For the $G-$modules $E(K),E(F),R_D(F),T_D(F)$ and $N_D(F)$, we have the following results about their corresponding cohomology groups:

Proposition 2.4. $\mathrm{H}^1(G,E(K))=R_D(F)/T_D(F)$; $\quad\mathrm{H}^1(G,E(F))=E(F)[2]$; $\mathrm{H}^1(G,R_D(F))=R_D(F)/2R_D(F)$; $\quad\mathrm{H}^1(G,T_D(F))=T_D(F)/2T_D(F)$; $\mathrm{H}^1(G,N_D(F))=N_D(F)[2]$.

Proof. Since G is cyclic, by the explicit formulae of cohomology of finite cyclic

groups (See [Se], pp.133, 128 for the details), we have

$$\mathrm{H}^1(G, E(K)) = \ker\varphi_1/\mathrm{im}\varphi_2 = R_D(F)/T_D(F);$$

$$\mathrm{H}^1(G, E(F)) = \ker(\varphi_1|E(F))/\mathrm{im}(\varphi_2|E(F)) = E(F)[2];$$

$$\mathrm{H}^1(G, R_D(F)) = \ker(\varphi_1|R_D(F))/\mathrm{im}(\varphi_2|R_D(F)) = R_D(F)/2R_D(F);$$

$$\mathrm{H}^1(G, T_D(F)) = \ker(\varphi_1|T_D(F))/\mathrm{im}(\varphi_2|T_D(F)) = T_D(F)/2T_D(F);$$

$$\mathrm{H}^1(G, N_D(F)) = \ker(\varphi_1|N_D(F))/\mathrm{im}(\varphi_2|N_D(F)) = N_D(F)[2].$$

This proves Proposition 2.4. $\square$

Theorem 2.5. The order of the group $\mathrm{H}^1(G, E(K))$ is

$$\begin{aligned}\sharp\mathrm{H}^1(G, E(K)) &= \frac{2^{r_{D,F}} \cdot \sharp E(F)[2]}{(E(K) : E(F) + R_D(F))} = \frac{2^{r_{D,F}} \cdot \sharp E(F)[2]}{(N_D(F) : 2E(F))} \\ &= 2^{r_{D,F} - r_F} \cdot (E(F) : N_D(F)).\end{aligned}$$

Proof. Let $A = R_D(F), B = E(K)$ and $C = N_D(F)$, their corresponding Herbrand quotients are

$$h(A) = h_0(A)/h_1(A),\ h(B) = h_0(B)/h_1(B),\ h(C) = h_0(C)/h_1(C),$$

where $h_m(\cdot)$ is the order of $\widehat{\mathrm{H}}^m(G, \cdot)$ $(m = 0, 1)$ (see [AW], p. 109). Since $2E(F) \subset N_D(F) \subset E(F)$, $\mathrm{rank}E_D(F) = \mathrm{rank}R_D(F)$ and $\mathrm{rank}N_D(F) = \mathrm{rank}E(F)$, by Lemma 2.2 and Proposition 2.4, we have

$$\begin{aligned}h(R_D(F)) &= \frac{\sharp(R_D(F)^G/\varphi_1(R_D(F)))}{\sharp\mathrm{H}^1(G, R_D(F))} = \frac{\sharp E(F)[2]}{\sharp(R_D(F)/2R_D(F))} = 2^{-r_{D,F}}, \\ h(E(K)) &= \frac{\sharp(E(K)^G/\varphi_1(E(K)))}{\sharp\mathrm{H}^1(G, E(K))} = \frac{\sharp(E(F)/N_D(F))}{\sharp\mathrm{H}^1(G, E(K))} \\ &= \frac{2^{r_F} \cdot \sharp E(F)[2]}{\sharp\mathrm{H}^1(G, E(K)) \cdot (N_D(F) : 2E(F))}, \\ h(N_D(F)) &= \frac{\sharp(N_D(F)^G/\varphi_1(N_D(F)))}{\sharp\mathrm{H}^1(G, N_D(F))} = \frac{\sharp(N_D(F)/2N_D(F))}{\sharp N_D(F)[2]} = 2^{r_F}.\end{aligned}$$

Since $O \longrightarrow R_D(F) \longrightarrow E(K) \longrightarrow^{\varphi_1} N_D(F) \longrightarrow O$ is an exact sequence of $G-$modules, by the theorem of Herbrand quotient (see [AW], Prop.10 on p.109), we have $h(E(K)) = h(R_D(F)) \cdot h(N_D(F))$. Therefore by the above calculation and Lemma 2.3, we get

$$\sharp \mathrm{H}^1(G, E(K)) = \frac{2^{r_{D,F}} \cdot \sharp E(F)[2]}{(N_D(F) : 2E(F))} = \frac{2^{r_{D,F}} \cdot \sharp E(F)[2]}{(E(K) : E(F) + R_D(F))}$$
$$= 2^{r_{D,F} - r_F} \cdot (E(F) : N_D(F)).$$

This proves Theorem 2.5. $\square$

Corollary 2.6. If $r_F = 0$ and $E(F)[2] = \{O\}$, then $E(K) = E(F) + R_D(F)$ and $\sharp \mathrm{H}^1(G, E(K)) = 2^{r_{D,F}} = 2^{r_K}$.

Proof. If $r_F = 0$ and $E(F)[2] = \{O\}$, then by the Mordell-Weil theorem, $E(F)/2E(F) \cong (\mathbb{Z}/2\mathbb{Z})^{r_F} \oplus E(F)[2] = 0$. So $(N_D(F) : 2E(F)) = 1$ because $N_D(F)/2E(F) \subset E(F)/2E(F)$, and then the conclusions follow from Lemma 2.3 and Theorem 2.5. This proves corollary 2.6. $\square$

3. The Shafarevich-Tate groups upon quadratic extension

For the quadratic extension K/F of number fields and the elliptic curve E (over F) as above, write M_F (resp. M_K) for a complete set of places on F (resp. K), let S_∞ be the set of infinite (i.e., Archimedean) places of F and S be the set of finite places of F obtained by collecting together all places that ramify in K/F and all places of bad reduction for E/F. Fix a place $w \in M_K$ lying above v for each $v \in M_F$. Denote $\mathrm{Gal}(K_w/F_v)$ by G_w, where F_v and K_w are the completions of F at v and K at w, respectively. The discriminant of the elliptic curve E over F is denoted by $\Delta(E)$. In the following, we set

$S_{\infty,1} = \{\text{all real places of } F\} \subset S_\infty$;

$S_0 = \{v \in S : \ v \text{ is ramified or inertial in } K\}$;

$S_g = \{v \in S_0 : \ v \nmid 2 \text{ and } E \text{ has good reduction at } v\}$;

$S_{gu} = \{v \in S_0 : \ v \mid 2, \ E \text{ has good reduction at } v \text{ and } F_v \text{ is unramified over } \mathbb{Q}_2\}$;

$S_{ar} = \{v \in S_0 : \ E \text{ has additive reduction at } v\}$;

$S_a = S_{ar} \cup \{v \in S_0 : \ v \mid 2, \ E \text{ has good reduction at } v \text{ and } F_v \text{ is ramified over } \mathbb{Q}_2\}$;

$S_{smr} = \{v \in S_0 : \ E \text{ has split multiplicative reduction at } v\}$;

$S_{nsmr} = \{v \in S_0 : \ E \text{ has non-split multiplicative reduction at } v\}$

$= S'_{nsmr} \sqcup S''_{nsmr}$ (the disjoint union), where

$S'_{nsmr} = \{v \in S_{nsmr} : \ v \text{ is inertial in } K\}$,

$S''_{nsmr} = \{v \in S_{nsmr} : \ v \text{ is ramified in } K\}$.

Obviously, $S_0 = S_g \sqcup S_{gu} \sqcup S_a \sqcup S_{smr} \sqcup S_{nsmr}$ (the disjoint union). For each $v \in S_{\infty,1}$, let $\sigma_v : F \to F_v = \mathbb{R}$ be the corresponding real embedding, so $\sigma_v(a) \in \mathbb{R}$ for any $a \in F$. For each finite place v of F, we use $v(\cdot)$ to denote the normalized additive valuation of F_v, i.e., $v(F_v^*) = \mathbb{Z}$. Let $\| a \|_{F_v} = (\sharp k_v)^{-v(a)}$ $(a \in F_v)$ denote the absolute value on F_v (k_v is the residue field of F_v), so is the meaning of $\| a \|_{K_w}$ on K_w. Let $\Delta_v, \Delta_{D,v}$, and Δ_w be the minimal discriminants for E over F_v, E_D over F_v and E over K_w (see [Si1]), let $c_v, c_{D,v}$ and c_w be the fudge factors (or Tamagawa factors) for E over F_v, E_D over F_v and E over K_w (see [R 3]), and let $d(K_w/F_v)$ be the discriminant of K_w/F_v, determined up to the square of a unit of F_v (see [KT], p. 332). We also let $(\ , \ )_{F_v}$ denote the Hilbert norm-residue symbol, a bimultiplicative form $(\ , \ )_{F_v} : \ F_v^* \times F_v^* \to \mu_2 = \{1, -1\}$ whose properties are described in [Se]. For a vector space V over $\mathbb{F}_2$, the finite field with $2-$elements, we denote its dimension

by $\dim_2 V$.

Definition 3.1. We denote $\delta(E,F,K)=\delta_\infty+\delta_f$, where

$\delta_\infty=\sharp\{v\in S_{\infty,1}:\ v$ is ramified in K and $\sigma_v(\Delta(E))>0\}$, and

$$\delta_f=\sum_{v\in S_0}\log_2\left(\frac{c_v c_{D,v}}{c_w}\left(\frac{\parallel \Delta_v\Delta_{D,v}d(K_w/F_v)^{-6}\parallel_{F_v}}{\parallel \Delta_w\parallel_{K_w}}\right)^{1/12}\right).$$

We call $\delta(E,F,K)$ the Mazur-Kramer-Tunnell index (for short, the MKT index) of E over K/F (for an arithmetic meaning of each term of the above summation, see [KT, p.332] and [Ma, pp. 203, 204]). By the results of Kramer on the local norm index in [Kr], one can calculate δ_f alternatively for most cases as follows:

$\delta_f=\delta_g+\delta_m+\delta_a$, where δ_g,δ_m and δ_a are defined as follows:

$$\delta_a=\sum_{v\in S_a}\dim_2(E(F_v)/N(K_w));$$

$$\delta_m=\delta_{smr}+\delta_{nsmr} \text{ with } \delta_{smr}=\frac{1}{2}\sum_{v\in S_{smr}}(1+(\Delta_v,D)_{F_v}) \text{ and}$$

$$\delta_{nsmr}=\frac{1}{2}\sum_{v\in S'_{nsmr}}\left(1+(-1)^{v(\Delta_v)}\right)+\sum_{v\in S''_{nsmr}}\left(\frac{1}{2}(1+(\Delta_v,D)_{F_v})\cdot(-1)^{v(\Delta_v)}+1\right);$$

$$\delta_g=\sum_{v\in S_g}\dim_2\widetilde{E_v}(k_v)[2]+\sum_{v\in S_{gu}}\varepsilon(v), \text{where}$$

$$\varepsilon(v)=\begin{cases}\frac{1}{2}\left(1-(-1)^{v(D)}\right)\cdot[F_v:\mathbb{Q}_2] & \text{if } E \text{ has good supersingular reduction at } v,\\ \frac{1}{2}(3+(\Delta_v,D)_{F_v}) & \text{if } E \text{ has good ordinary reduction at } v.\end{cases}$$

Here $\widetilde{E_v}$ is the reduction of E at v, k_v is the residue field of F_v. Note that δ_a is usually most difficult to compute (see [Kr]).

Now for the Shafarevich-Tate groups Ш(E/F), Ш(E_D/F) and Ш(E/K), we have

Theorem 3.2. Assume that the Shafarevich-Tate groups are finite. Then

$$\frac{\sharp\,\text{Ш}(E/F)\cdot\sharp\,\text{Ш}(E_D/F)}{\sharp\,\text{Ш}(E/K)}=2^{r_{D,F}-r_F-\delta(E,F,K)}\cdot(E(F):N_D(F))^2,$$

where $\delta(E,F,K)$ is the MKT index of E over K/F.

Proof. By the Main Theorem of [Y], we have

$$\frac{\sharp\,\text{Ш}(E/F)\cdot\sharp\,\text{Ш}(E_D/F)}{\sharp\,\text{Ш}(E/K)}=\frac{\sharp\widehat{\mathrm{H}}^0(G,E(K))\cdot\sharp\mathrm{H}^1(G,E(K))}{\prod_{v\in M_F}\sharp\mathrm{H}^1(G_w,E(K_w))}.$$

By definition (see [Se]), $\widehat{\mathrm{H}}^0(G,E(K))=E(K)^G/(1+\sigma)E(K)=E(F)/N_D(F)$, so by the above Theorem 2.5, we get

$$\frac{\sharp\,\text{Ш}(E/F)\cdot\sharp\,\text{Ш}(E_D/F)}{\sharp\,\text{Ш}(E/K)}=\frac{2^{r_{D,F}-r_F}\cdot(E(F):N_D(F))^2}{\prod_{v\in M_F}\sharp\mathrm{H}^1(G_w,E(K_w))}.$$

On the other hand, by the Lemma 2.3 in [GA], we have $\mathrm{H}^1(G_w,E(K_w))=0$ for any $v\notin S\cup S_\infty$. Therefore

$$\frac{\sharp\,\text{Ш}(E/F)\cdot\sharp\,\text{Ш}(E_D/F)}{\sharp\,\text{Ш}(E/K)}=\frac{2^{r_{D,F}-r_F}\cdot(E(F):N_D(F))^2}{\prod_{v\in S\cup S_\infty}\sharp\mathrm{H}^1(G_w,E(K_w))}. \tag{3.1}$$

By our assumption, the Shafarevich-Tate groups are finite, also $(E(F):N_D(F))<\infty$ because $\mathrm{rank}E(F)=\mathrm{rank}N_D(F)$, so by the above formula (3.1), $\mathrm{H}^1(G_w,E(K_w))$ is a finite set for each $v\in S\cup S_\infty$.

Let $v\in S_\infty$, if v is unramified in K, then $\mathrm{H}^1(G_w,E(K_w))=0$ because $K_w=F_v=\mathbb{R}$ or $\mathbb{C}$. So we may assume that $v\in S_{\infty,1}$ and v is ramified in K, then $F_v=\mathbb{R}$ and $K_w=\mathbb{C}$. By the Theorem 2.4 of Chapter V in [Si2], we have

$$\mathrm{H}^1(G_w,E(K_w))=\mathrm{H}^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),E(\mathbb{C}))\cong\begin{cases}0 & \text{if } \sigma_v(\Delta(E))<0,\\ \mathbb{Z}/2\mathbb{Z} & \text{if } \sigma_v(\Delta(E))>0.\end{cases}$$

Hence

$$\prod_{v\in S_\infty}\sharp\mathrm{H}^1(G_w,E(K_w))=\sharp\,(\mathbb{Z}/2\mathbb{Z})^{\delta_\infty}=2^{\delta_\infty}. \tag{3.2}$$

Let $v\in S$, if $v\notin S_0$, then v splits completely in K, so $K_w=F_v$ and then $\mathrm{H}^1(G_w,E(K_w))=0$. For $v\in S_0$, since $\mathrm{H}^1(G_w,E(K_w))$ is finite as mentioned above,

by Proposition 4.2 of [Ma], we have $\sharp \mathrm{H}^1(G_w, E(K_w)) = (E(F_v) : N(K_w))$. Hence by the Theorem 7.6 and the Remark in [KT, pp. 332, 333] (or by Prop.1 $\sim$ 5 in [Kr]), we get

$$\prod_{v\in S} \sharp \mathrm{H}^1(G_w, E(K_w)) = \prod_{v\in S_0} \sharp \mathrm{H}^1(G_w, E(K_w)) = 2^{\delta_f}. \tag{3.3}$$

Substitute (3.2) and (3.3) into (3.1), we get

$$\frac{\sharp\, Ш(E/F) \cdot \sharp\, Ш(E_D/F)}{\sharp\, Ш(E/K)} = 2^{r_{D,F}-r_F-\delta(E,F,K)} \cdot (E(F) : N_D(F))^2.$$

This proves Theorem 3.2. $\square$

4. Shafarevich-Tate groups, congruent numbers and and BSD conjecture

Let $n \in \mathbb{Z} \setminus \{0, 1\}$ be a square free integer and $K = \mathbb{Q}(\sqrt{n})$ be a quadratic number field. In this section, we consider elliptic curves $E : y^2 = x^3 - x$ and $E_n : y^2 = x^3 - n^2x$. All these curves have complex multiplication by $\mathbb{Z}[\sqrt{-1}]$, the Gaussian integral ring. Let $w \in M_K$ be a place of K lying over 2, as in section 3 above, recall that the notations Δ_w and c_w represent the minimal discriminant and the fudge factor for E over K_w, respectively. Denote by ord_w the normalized additive valuation of K_w.

Lemma 4.1. We have

$$\mathrm{ord}_w(\Delta_w) = \begin{cases} 6 & \text{if } n \equiv 1 \pmod 4, \\ 12 & \text{if } n \equiv 2 \text{ or } 3 \pmod 4), \end{cases} \quad \text{and}$$

$$c_w = \begin{cases} 4 & \text{if } n \equiv 2 \text{ or } 7 \pmod 8, \\ 2 & \text{if } n \equiv 1, 3, 5 \text{ or } 6 \pmod 8). \end{cases}$$

Proof. It is well known that, up to isomorphisms, there are exactly seven quadratic extensions of $\mathbb{Q}_2$, namely, $\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{-2}), \mathbb{Q}_2(\sqrt{2}), \mathbb{Q}_2(\sqrt{-3}), \mathbb{Q}_2(\sqrt{3}),$ $\mathbb{Q}_2(\sqrt{-6}), \mathbb{Q}_2(\sqrt{-6})$ (see [W], p.248). Furthermore, one can easily verified that

$K_w \cong \mathbb{Q}_2 \Longleftrightarrow n \equiv 1 \pmod 8$; $K_w \cong \mathbb{Q}_2(\sqrt{-3}) \Longleftrightarrow n \equiv 5 \pmod 8$;

$K_w \cong \mathbb{Q}_2(\sqrt{-1}) \Longleftrightarrow n \equiv 7 \pmod 8$; $K_w \cong \mathbb{Q}_2(\sqrt{3}) \Longleftrightarrow n \equiv 3 \pmod 8$;

$K_w \cong \mathbb{Q}_2(\sqrt{-2}) \Longleftrightarrow n \equiv 14 \pmod{16}$; $K_w \cong \mathbb{Q}_2(\sqrt{2}) \Longleftrightarrow n \equiv 2 \pmod{16}$;

$K_w \cong \mathbb{Q}_2(\sqrt{-6}) \Longleftrightarrow n \equiv 10, 26 \text{ or } 42 \pmod{48}$;

$K_w \cong \mathbb{Q}_2(\sqrt{6}) \Longleftrightarrow n \equiv 6, 22 \text{ or } 38 \pmod{48}$.

Next, by Tate's algorithm (see [Ta], [Si2]), after a tedious calculation, we get

$$c_w = \begin{cases} 2 & \text{if } K_w = \mathbb{Q}_2, \mathbb{Q}_2(\sqrt{-3}), \mathbb{Q}_2(\sqrt{-2}), \mathbb{Q}_2(\sqrt{3}) \text{ or } \mathbb{Q}_2(\sqrt{6}), \\ 4 & \text{if } K_w = \mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{2}) \text{ or } \mathbb{Q}_2(\sqrt{-6}), \quad \text{and} \end{cases}$$

$$\mathrm{ord}_w(\Delta_w) = \begin{cases} 6 & \text{if } n \equiv 1 \pmod 4, \\ 12 & \text{if } n \equiv 2 \text{ or } 3 \pmod 4, \end{cases}$$

from which the conclusion follows, and the proof is completed. □

Then we compute the MKT index $\delta(E, \mathbb{Q}, K)$ of E over $K/\mathbb{Q}$ as follows:

Lemma 4.2. We have

$$\delta(E, \mathbb{Q}, K) = \begin{cases} 2\omega_0(n) & \text{if } n > 0 \text{ and } n \equiv 1 \pmod 8, \\ 1 + 2\omega_0(n) & \text{if } n > 0 \text{ and } n \equiv 5 \text{ or } 7 \pmod 8, \\ 3 + 2\omega_0(n) & \text{if } n > 0 \text{ and } n \equiv 6 \pmod 8, \\ 2 + 2\omega_0(n) & \text{if } n > 0 \text{ and } n \equiv 2 \text{ or } 3 \pmod 8, \\ 1 + 2\omega_0(n) & \text{if } n < 0 \text{ and } n \equiv 1 \pmod 8, \\ 2 + 2\omega_0(n) & \text{if } n < 0 \text{ and } n \equiv 5 \text{ or } 7 \pmod 8, \\ 3 + 2\omega_0(n) & \text{if } n < 0 \text{ and } n \equiv 2 \text{ or } 3 \pmod 8, \\ 4 + 2\omega_0(n) & \text{if } n < 0 \text{ and } n \equiv 6 \pmod 8, \end{cases}$$

where $\omega_0(n)$ is the number of odd prime divisors of n.

Proof. Since $\Delta(E) = 64 > 0$, E has good reduction everywhere except at 2 with additive reduction. So, by definition, $S_{\infty,1} = \{\infty\}$, $S = \{2\} \cup \{p : p \text{ is a prime and } p \mid n\}, S_{gu} = S_{smr} = S_{nsmr} = \emptyset$ and $S_g = S \setminus \{2\}$. So $\delta_m = 0$, and $\delta_\infty = 0$ (resp., 1) if $n > 0$ (resp., $n < 0$). Moreover, for each odd prime p, E has good reduction at p, and it easy to see that $\widetilde{E}(\mathbb{F}_p)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$, so $\delta_g = \sum_{p \in S_g} \dim_2 \widetilde{E}(\mathbb{F}_p)[2] = 2\omega_0(n)$. Hence by definition, $\delta(E, \mathbb{Q}, K) = \delta_\infty + \delta_g +$

$\delta_m + \delta_a = 2\omega_0(n) + \delta_\infty + \delta_a$. We divide our discussion into the following cases.

Case A. $n \equiv 1 \pmod 8$. Then 2 splits completely in K, and then $S_a = \emptyset$, so $\delta_a = 0$, which implies $\delta(E, \mathbb{Q}, K) = 2\omega_0(n)$ (resp., $2\omega_0(n) + 1$) if $n > 0$ (resp., $n < 0$).

Case B. $n \equiv 2, 3, 5, 6$ or $7 \pmod 8$. Then 2 is ramified or inertial in K, so $S_a = \{2\}$. Let $w \in M_K$ be the unique place in K lying above 2, then $K_w = \mathbb{Q}_2(\sqrt{n})$ is a quadratic extension over $\mathbb{Q}_2$. By Def.3.1 above and the Thm.7.6 in [KT], we get

$$\delta_a = \dim_2(E(\mathbb{Q}_2)/N(K_w)) = \log_2 \left(\frac{c_2 c_{n,2}}{c_w} \left(\frac{\| \Delta_2 \Delta_{n,v} d_w^{-6} \|_{\mathbb{Q}_2}}{\| \Delta_w \|_{K_w}} \right)^{1/12} \right). \tag{4.1}$$

Now we only need to compute all the values of $c_2, c_{n,2}, c_w, \Delta_2, \Delta_{n,v}, \Delta_w$ and d_w. Firstly, by a method in ([KT], p.331) it is easy to see that

$$d_w = d(K_w/\mathbb{Q}_2) = \begin{cases} n & \text{if } n \equiv 5 \pmod 8, \\ 4n & \text{if } n \equiv 2 \text{ or } 3 \pmod 4). \end{cases}$$

Next, for the elliptic curves E and E_n over $\mathbb{Q}_2$, by Tate's algorithm (see [Ta], [Si2], [R3]), one can easily obtain that $v_2(\Delta_2) = 6,\ c_2 = 2$ and

$v_2(\Delta_{n,2}) = 6$ if $n \equiv 3, 5$ or $7 \pmod 8$; $v_2(\Delta_{n,2}) = 12$ if $n \equiv 2$ or $6 \pmod 8$;

$c_{n,2} = 2$ if $n \equiv 3, 5$ or $7 \pmod 8$; $c_{n,2} = 4$ if $n \equiv 2$ or $6 \pmod 8$.

Also by Lemma 4.1 above, we have

$\mathrm{ord}_w(\Delta_w) = 12$ if $n \equiv 2$ or $3 \pmod 4$; $\mathrm{ord}_w(\Delta_w) = 6$ if $n \equiv 5 \pmod 8$;

$c_w = 2$ if $n \equiv 3, 5$ or $6 \pmod 8$; $c_w = 4$ if $n \equiv 2$ or $7 \pmod 8$.

Now substitute all of them into (4.1), the conclusion for case B then follows, and the proof is completed. $\square$

For the groups of $E(\mathbb{Q}(\sqrt{n}))$ and $E_n(\mathbb{Q})$, we have the following results:

Theorem 4.3. Let n be a square free integer satisfying one of the following conditions

(1) $n > 0$ and $n \equiv 5, 6$ or $7 \pmod 8$; (2) $n < 0$ and $n \equiv 1, 2$ or $3 \pmod 8$.

Then for the elliptic curves E and E_n as above, if both $Ш(E_n/\mathbb{Q})$ and $Ш(E/\mathbb{Q}(\sqrt{n}))$ are finite, we have

$$\mathrm{rank}(E(\mathbb{Q}(\sqrt{n}))) = \mathrm{rank}(E_n(\mathbb{Q})) \equiv 1 \pmod 2.$$

In particular, both $E(\mathbb{Q}(\sqrt{n}))$ and $E_n(\mathbb{Q})$ are infinite groups.

Proof. For each n satisfying the given condition, by the above Lemma 4.2, we know that the conrresponding MKT index $\delta(E, \mathbb{Q}, K)$ is odd. Since $\mathrm{rank}(E(\mathbb{Q})) = 0$ and $Ш(E/\mathbb{Q}) = 0$ (see e.g., [R1]), by the above Corollary C we get $\mathrm{rank}(E(\mathbb{Q}(\sqrt{n}))) \equiv \mathrm{rank}(E_n(\mathbb{Q})) - \mathrm{rank}(E(\mathbb{Q})) \equiv 1 \pmod 2$, which implies the conclusion, and the proof is completed. $\square$

For the Shafarevich-Tate groups $Ш\,(E/\mathbb{Q}(\sqrt{n}))$ and the BSD conjecture for $E/\mathbb{Q}(\sqrt{n})$, we have the following results:

Theorem 4.4. Let n be a square free integer satisfying one of the following conditions

(1) $n > 0$ and $n \equiv 1, 2$ or $3 \pmod 8$; (2) $n < 0$ and $n \equiv 5, 6$ or $7 \pmod 8$.

Then for the elliptic curves $E = E_1 : y^2 = x^3 - x$ and E_n as above, if the full BSD conjecture is true for E_n over $\mathbb{Q}$ with $L(E_n/\mathbb{Q}, 1) \neq 0$, and $Ш\,(E/\mathbb{Q}(\sqrt{n}))$ is finite, we have

$$\sharp\,Ш(E/\mathbb{Q}(\sqrt{n})) = \begin{cases} 2^{-4} \cdot a_n^2 & \text{if } n > 0 \text{ and } n \equiv 1 \pmod 8, \\ 2^{-2} \cdot a_n^2 & \text{if } n > 0 \text{ and } n \equiv 3 \pmod 8, \\ 2^{-2} \cdot (a'_{n/2})^2 & \text{if } n > 0 \text{ and } n \equiv 2 \pmod 8, \\ 2^{-2} \cdot a_{-n}^2 & \text{if } n < 0 \text{ and } n \equiv 5 \text{ or } 7 \pmod 8, \\ (a'_{-n/2})^2 & \text{if } n < 0 \text{ and } n \equiv 6 \pmod 8, \end{cases}$$

where $a_{|n|}$ and $a'_{|n/2|}$ are the Fourier coefficients of the above modular forms f and f'. Moreover, the full BSD conjecture is true for E over the quadratic field $\mathbb{Q}(\sqrt{n})$.

Proof. We prove the case that $n>0$ satisfying $n \equiv 1 \pmod 8$, the other cases can be similarly verified. For this case, by Lemma 4.2 above, the conrresponding MKT index $\delta(E,\mathbb{Q},K) = 2\omega_0(n)$. By the assumption, $L(E_n/\mathbb{Q},1) \neq 0$ and the full BSD conjecture is true for E_n over $\mathbb{Q}$, so $r_{n,\mathbb{Q}} = 0$, Ш $(E_n/\mathbb{Q})$ is finite and $L(E_n/\mathbb{Q},1)/\Omega_{E_n/\mathbb{Q}} = (\mathrm{BSD})_{\infty,\mathbb{Q}}(E_n)$ with $\Omega_{E_n/\mathbb{Q}} = \omega/\sqrt{n}$, where

$$(\mathrm{BSD})_{\infty,\mathbb{Q}}(E_n) = \mathrm{Reg}_{\infty,\mathbb{Q}}(E_n) \times \frac{\sharp\, Ш(E_n/\mathbb{Q}) \prod_{v\in M_{\mathbb{Q}}} c_v}{\sqrt{d(\mathbb{Q})} \times \sharp E_n(\mathbb{Q})^2_{\mathrm{tors}}}.$$

We have $\mathrm{Reg}_{\infty,\mathbb{Q}}(E_n) = 1$ because $r_{n,\mathbb{Q}} = 0$; obviously, $d(\mathbb{Q}) = 1$; also $\sharp E_n(\mathbb{Q})_{\mathrm{tors}} = 4$ (see [Si1], pp.346, 347); moreover, $c_\infty = 2$ because E_n is not connected over $\mathbb{R}$, then from [R3] we have

$$\prod_{v\in M_{\mathbb{Q}}} c_v = c_\infty \cdot \prod_{p<\infty} c_p = 2 \times 2^{2\omega_0(n)+1} = 2^{2\omega_0(n)+2}, \quad \text{hence}$$

$$L(E_n/\mathbb{Q},1) = \Omega_{E_n/\mathbb{Q}} \times (\mathrm{BSD})_{\infty,\mathbb{Q}}(E_n) = 2^{2\omega_0(n)-2} \times \frac{\omega}{\sqrt{n}} \times \sharp\, Ш(E_n/\mathbb{Q}). \quad (4.2)$$

On the other hand, by Tunnell's theorem (see [T], [Kob]), we have $L(E_n/\mathbb{Q},1) = \omega a_n^2/(4\sqrt{n})$ with the Fourier coefficient a_n of the modular form f mentioned above. Therefore by (4.2), we get $\sharp\, Ш(E_n/\mathbb{Q}) = 2^{-2\omega_0(n)} \cdot a_n^2$. As mentioned before, Ш$(E/\mathbb{Q}) = 0$, and $E(\mathbb{Q}) = E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$, so $r_K = r_{n,\mathbb{Q}} + r_{\mathbb{Q}} = 0$, and it is easy to know that $E(K)_{tors} = E(\mathbb{Q})[2]$, hence by definition, we have $(E(\mathbb{Q}) : N_n(\mathbb{Q})) = 4$.

By assumption, Ш $(E/\mathbb{Q}(\sqrt{n}))$ is finite, hence by Theorem 3.2 above, we get

$$\sharp\,Ш(E/\mathbb{Q}(\sqrt{n})) = 2^{-r_{n,\mathbb{Q}}+r_{\mathbb{Q}}+\delta(E,\mathbb{Q},K)} \cdot (E(\mathbb{Q}) : N_n(\mathbb{Q}))^{-2} \cdot \sharp\,Ш(E/\mathbb{Q}) \cdot \sharp\,Ш(E_n/\mathbb{Q})$$

$$= 2^{2\omega_0(n)} \cdot 4^{-2} \cdot 2^{-2\omega_0(n)} \cdot a_n^2 = 2^{-4}a_n^2. \quad \text{In particular,}$$

$$\frac{\sharp\,Ш(E/\mathbb{Q}(\sqrt{n}))}{\sharp\,Ш(E_n/\mathbb{Q})} = 2^{2\omega_0(n)-4}.$$

Therefore the conclusion of the Shafarevich-Tate groups Ш $(E/\mathbb{Q}(\sqrt{n}))$ is obtained.

Next we come to verify the full BSD conjecture for E over $K = \mathbb{Q}(\sqrt{n})$. Since $r_K = 0$, $L(E/\mathbb{Q}, 1) = \omega/4$ (see [R1]) and $L(E/K, 1) = L(E/\mathbb{Q}, 1) \cdot L(E_n/\mathbb{Q}, 1) \neq 0$, we only need to show that

$$L(E/K, 1) = \Omega_{E/K} \times (\mathrm{BSD})_{\infty,K}(E), \tag{4.3}$$

$$\text{where} \quad (\mathrm{BSD})_{\infty,K}(E) = \mathrm{Reg}_{\infty,K}(E) \times \frac{\sharp\,Ш(E/K)\prod_{w\in M_K} c_w}{\sqrt{d(K)} \times \sharp E(K)^2_{\mathrm{tors}}}.$$

To see this, firstly, the discriminant $d(K) = n$ and $\mathrm{Reg}_{\infty,K}(E) = 1$ because $r_K = 0$; also, by definition, it is easy to know that $\Omega_{E/K} = \omega^2$ (see[D], p.22). Since 2 is split in K, there are two places w_1, w_2 of K lying over 2, and by Lemma 4.1 above, we have $c_{w_1} = c_{w_2} = 2$. Note that, over K, E has good reduction everywhere except at the places w_1 and w_2, hence $\prod_{w\in M_K \text{ and } w<\infty} c_w = \prod_{w|2} c_w = c_{w_1} \cdot c_{w_2} = 4$; Moreover, since K is real, there are two real embeddings $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{R}$, so $\prod_{w|\infty} c_w = c_{1,\infty} \cdot c_{2,\infty} = 2 \times 2 = 4$. Therefore, together with the above result of Ш (E/K), we have

$$(\mathrm{BSD})_{\infty,K}(E) = \mathrm{Reg}_{\infty,K}(E) \times \frac{\sharp\,Ш(E/K)\prod_{w\in M_K} c_w}{\sqrt{d(K)} \times \sharp E(K)^2_{\mathrm{tors}}}$$

$$= 1 \times \frac{2^{-4}a_n^2 \cdot \prod_{w|\infty} c_w \cdot \prod_{w|2} c_w}{\sqrt{n} \cdot 16}$$

$$= \frac{a_n^2}{16\sqrt{n}}.$$

On the other hand, by the above discussion we have

$$\begin{aligned} L(E/K,1) &= L(E/\mathbb{Q},1)\cdot L(E_n/\mathbb{Q},1) = \frac{\omega}{4}\cdot\frac{\omega}{4\sqrt{n}}\cdot a_n^2 \\ &= \frac{\omega^2}{16\sqrt{n}}\cdot a_n^2 = \omega^2\cdot(\mathrm{BSD})_{\infty,K}(E) = \Omega_{E/K}\times(\mathrm{BSD})_{\infty,K}(E). \end{aligned}$$

Therefore the equality of (4.3) holds, this proves the full BSD conjecture for E over K, and the proof of Theorem 4.4 is completed. $\square$

5. Shafarevich-Tate groups and Heegner points.

In this section, let E be an elliptic curve defined over $\mathbb{Q}$, N_E be the conductor of $E/\mathbb{Q}$, let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field with fundamental discriminant D satisfying the Heegner hypothesis, that is,

Heegner hypothesis. All prime numbers p dividing N_E are split in K.

Then there exists a Heegner point $P_K \in E(K)$ (see [GZ], [Kol1∼3]). We have the following results of Shafarevich-Tate groups and Heegner points:

Theorem 5.1. (1) Let E be an elliptic curve defined over $\mathbb{Q}$, and $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field satisfying the Heegner hypothesis. Let P_K be a Heegner point of $E(K)$, if P_K is of infinite order, then

$$\frac{\sharp\,Ш(E/\mathbb{Q})\cdot\sharp\,Ш(E_D/\mathbb{Q})}{\sharp\,Ш(E/K)} = \begin{cases} 2^{1-\delta_\infty-\delta_g}\cdot(E(\mathbb{Q}):N_D(\mathbb{Q}))^2 & \text{if } L(E/\mathbb{Q},1)\neq 0, \\ 2^{-1-\delta_\infty-\delta_g}\cdot(E(\mathbb{Q}):N_D(\mathbb{Q}))^2 & \text{if } L(E/\mathbb{Q},1)=0. \end{cases}$$

(2) For the elliptic curve $E: y^2 = x^3 - x + \frac{1}{4}$ and the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ satisfying the Heegner hypothesis, if the Heegner point $P_K \in E(K)$ is of infinite order, then

$$\sharp\,Ш(E/K) = 2^{\delta_g}\cdot\sharp\,Ш(E_D/\mathbb{Q}).$$

In particular, for each $D \in \{-7, -11, -47, -71, -83, -84, -127, -159, -164, -219, -231, -263, -271, -287, -292, -303, -308, -359, -371, -404, -443, -447, -471\}$, the group Ш (E/K) is trivial.

Proof. (1) For the elliptic curve $E/\mathbb{Q}$ and the field K, by definition, $S_{\infty,1} = \{\infty\}$ and $S = \{p : p \text{ is a prime number and } p \mid DN_E\}$. By the Heegner hypothesis, N_E is prime to D, and $S_0 = \{p : p \text{ is a prime number and } p \mid D\}$, in particularly, E has good reduction at each prime $p \in S_0$, so $S_g \cup S_{gu} = S_0$, and then $S_a = S_{smr} = S_{nsmr} = \emptyset$. Hence by definition, $\delta(E, \mathbb{Q}, K) = \delta_\infty + \delta_g$ with $\delta_\infty = 1$ (resp., 0) if $\Delta(E) > 0$ (resp. $\Delta(E) < 0$). On the other hand, by the Heegner hypothesis, from the functional equation it is easy to see that $L(E/K, 1) = 0$. Since the Heegner point P_K is of infinite order, by the formula of Gross-Zagier (see [GZ]), the analytic rank $\mathrm{ord}_{s=1} L(E/K, s) = 1$, which implies (see, e.g. [GZ])

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1 \quad \text{and} \quad L(E_D/\mathbb{Q}, 1) \neq 0; \quad \text{or}$$

$$\mathrm{ord}_{s=1} L(E_D/\mathbb{Q}, s) = 1 \quad \text{and} \quad L(E/\mathbb{Q}, 1) \neq 0.$$

Then by the theorems of Kolyvagin and Gross-Zagier (see [Kol1~3], [GZ]), we know that $r_{\mathbb{Q}} = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$ and $r_{D,\mathbb{Q}} = \mathrm{ord}_{s=1} L(E_D/\mathbb{Q}, s)$, moreover, all the groups Ш (E/K), Ш $(E/\mathbb{Q})$ and Ш $(E_D/\mathbb{Q})$ are finite. The conclusion then follows directly from the above Theorem 3.2. This proves (1).

(2) For the elliptic curve $E : y^2 = x^3 - x + \frac{1}{4}$, its discriminant $\Delta(E) = N_E = 37 > 0$, and the equation $y^2 + y = x^3 - x$ is a global minimal equation of E over $\mathbb{Q}$. By a theorem of Kolyvagin (see [Kol3], p.444), we know that $L(E/\mathbb{Q}, 1) = 0$, $r_{\mathbb{Q}} = 1$ and Ш $(E/\mathbb{Q}) = 0$, moreover, $E(\mathbb{Q}) = \mathbb{Z}P_0$ with $P_0 = (0, \frac{1}{2})$. Now from the proof of (1),

we have $\delta_\infty = 1$ because $\Delta(E) > 0$, then by the formula in (1), we get

$$\sharp\, Ш(E/K) = 2^{2+\delta_g} \cdot (E(\mathbb{Q}) : N_D(\mathbb{Q}))^{-2} \cdot \sharp\, Ш(E_D/\mathbb{Q}). \tag{5.1}$$

Since $E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times E(\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z}$ because $E(\mathbb{Q})[2] = 0$, by definition, $(E(\mathbb{Q}) : N_D(\mathbb{Q})) \mid (E(\mathbb{Q}) : 2E(\mathbb{Q})) = 2$, hence $N_D(\mathbb{Q}) = E(\mathbb{Q})$ or $2E(\mathbb{Q})$. But by the group law algorithm (see [Si1], p.53), it is not difficult to verify that $P_0 \notin N_D(\mathbb{Q})$, which implies $N_D(\mathbb{Q}) = 2E(\mathbb{Q})$, so $(E(\mathbb{Q}) : N_D(\mathbb{Q})) = 2$. Substituting it into (5.1), we get

$$\sharp\, Ш(E/K) = 2^{\delta_g} \cdot \sharp\, Ш(E_D/\mathbb{Q}). \tag{5.2}$$

This proves the first conclusion in (2).

Now we assume that D is one of the given 23 integers. Then by a theorem of Kolyvagin (see [Kol2], p.477), $Ш\,(E_D/\mathbb{Q}) = 0$. So we only need to compute δ_g. From the discussion in (1), we know that $S_g \cup S_{gu} = S_0$, moreover, it is easy to know that $S_{gu} = \{2\}$ if and only if D is even, otherwise, $S_{gu} = \emptyset$. Furthermore, it can be seen easily that E has good supersingular reduction at 2. Hence by definition, we have

$$\delta_g = \sum_{p \in S_0 \setminus \{2\}} \dim_2 \widetilde{E_p}(\mathbb{F}_p)[2] + \varepsilon(2)$$

with $\varepsilon(2) = \frac{1}{2}(1 - (-1)^{v_2(D)})$ (resp., 0) if D is even (resp., odd). Obviously, $\varepsilon(2) = 0$ for each of these 23 integers, and by calculation, it can be easily seen that $\widetilde{E_p}(\mathbb{F}_p)[2] = \{O\}$ for each $p \in S_0 \setminus \{2\}$, which implies $\delta_g = 0$. Therefore, by (5.2), we get $\sharp\, Ш(E/K) = \sharp\, Ш(E_D/\mathbb{Q}) = 1$, that is, $Ш\,(E/K)$ is trivial. This proves (2), and the proof of Theorem 5.1 is completed. $\square$

Acknowledgement. I would like to thank Professor John Coates for his telling me the result of Tim and Vladimir Dokchitser.

References

[**ABF**] J. Antoniadis, M. Bungert, G. Frey, Properties of twists of elliptic curves, J. reine angew. math. 405 (1990), 1-28.

[**AW**] M. Atiyah, C.T.C. Wall, Cohomology of groups, in: Algebraic Number Theory (J.W.S. Cassels and A. Frohlich, Eds.), pp.94-115, London: Academic Press, 1967.

[**CW**] J. Coates, A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, Invent. math., 39 (1977), 223-251.

[**D**] D. Delbourgo, Elliptic Curves and Big Galois Representations, Cambridge: Cambridge University Press, 2008.

[**Dok**] T. Dokchitser, V. Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares, to appear in Ann. Math..

[**GA**] C.D. Gonzalez-Aviles, On Tate-Shafarevich groups of Abelian varieties, Proceedings of the American Mathematical Society, 128 (2000), 953-961.

[**GZ**] B.H. Gross, D.B. Zagier, Heegner points and derivatives of $L-$series, Invent. math., 84 (1986), 225-320.

[**Kob**] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, 2nd Edition, New York: Springer-Verlag, 1993.

[**Kol1**] V.A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and Ш $(E/\mathbb{Q})$ for a subclass of Weil curves, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 522-540, 670-671; translation in Math. USSR-Izv. 32 (1989), 523-541.

[**Kol2**] V.A. Kolyvagin, The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 1154-1180, 1327; translation in Math. USSR-Izv. 33 (1989), 473-499.

[**Kol3**] V.A. Kolyvagin, Euler systems. In The Grothendieck Festschrift, Vol. II, 435-483, Progr. Math. 87, Birkhauser Boston, Boston, MA, 1990.

[**Kr**] K. Kramer, Arithmetic of elliptic curves upon quadratic extension, Transactions of the American Mathematical Society, 264 (1981), 121-135.

[**KT**] K. Kramer, J. Tunnell, Elliptic curves and local $\varepsilon-$factors, Compositio Math., 46 (1982), 307-352.

[**L1**] S. Lang, Algebraic Number Theory, 2nd Edition, New York: Springer-Verlag, 1994.

[**L2**] S. Lang, Algebra, 3rd Edition, New York: Springer-Verlag, 2002.

[**Ma**] B. Mazur, Rational points of Abelian varieties with values in towers of number fields, Invent. math., 18 (1972), 183-266.

[**R1**] K. Rubin, Tate-Shafarevich groups and $L-$functions of elliptic curves with complex multiplication, Invent. math., 89 (1987), 527-560.

[**R2**] K. Rubin, The main conjectures of Iwasawa theory for imaginary quadratic fields, Invent. math., 103 (1991), 25-68.

[**R3**] K. Rubin, Fudge factors in the Birch and Swinnerton-Dyer conjecture, in: Ranks of Elliptic Curves and Random Matrix Theory (J.B. Conrey, D.W.

Farmer, F. Mezzadri and N.C. Snaith Eds.), pp.233-236, Cambridge: Cambridge University Press, 2007.

[**RS**] K. Rubin, A. Silverberg, Rank frequencies for quadratic twists of elliptic curves, Experiment Math., 10 (2001), 559-569.

[**Se**] J. -P. Serre, Local fields, New York: Springer-Verlag, 1979.

[**Si1**] J. H. Silverman, The Arithmetic of Elliptic Curves, GTM 106, 2nd Edition, New York: Springer-Verlag, 2009.

[**Si2**] J. H. Silverman, Advanced topics in the Arithmetic of Elliptic Curves, GTM 151, New York: Springer-Verlag, 1999.

[**Ta**] J. Tate, Algorithm for determing the type of a singular fiber in an elliptic pencil, in: Modular functions of one variable, IV, (Proc. Internat. Summer School, Univ. Antwerp 1972), pp.33-52. Lecture Notes in Math. 476, Springer, Berlin, 1975.

[**T**] J. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, Invent. math., 72 (1983), 323-334.

[**W**] E. Weiss, Algebraic Number Theory, New York: McGraw-Hill Book C ompany, Inc, 1963.

[**Y**] H. Yu, On Tate-Shafarevich groups over Galois extensions, Israel J. Math., 141 (2004), 211-220.

[**Z**] C. Zhao, A criterion for elliptic curves with lowest 2-power in L(1), Math. Proc. Cambridge Philos. Soc. 121(1997), 385-400.